Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Remote Administration of Internal Devices Standard

Category	**Security Architecture**
Title	**Remote Administration of Internal Devices Standard**
Number	

Applicability

☑ State Government Agencies
- ☐ **All**.....Not Applicable
- ☑ **Excluding higher education institutions**.....**Standard**

☐ State Funded Entities - **All entities receiving state funding for matters covered by this document**.....Not Applicable

☐ Other: **All Public Entities**.....Not Applicable

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval as outlined in section 3.2
Guideline - Adherence is voluntary.

Status	☑ **Adopted** ☐ **Draft** ☐ **Other:**_____
Dates	**Date: April 3, 2007** **Date Adopted by NITC: June 27, 2007** **Other:**

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard

It is the responsibility of all State of Nebraska agencies to strictly control remote access from any device that connects from inside the State of Nebraska network to a desktop, server or network device elsewhere within the State of Nebraska network (e.g. from a 10.x.x.x device to a 10.x.x.x device) and ensure that employees, contractors, vendors and any other agent granted remote access privileges adhere to common methods of secure remote administration which shall include but are not limited to:

- Use of strong authentication mechanisms (e.g., strong passwords, public/private key pair, two factor authentication, etc.)
- Utilize device host access (by IP address) lists to restrict remote access
- Use of secure protocols that provide encryption of both passwords and data (e.g., SSL, HTTPS) when reasonable and appropriate, rather than insecure protocols (e.g., Telnet, FTP).
- Grant permissions to only those with a job related need.
- Implement the 'Principle of Least Privilege' to those who are granted permissions.
- Reset factory default device passwords and regularly change any default accounts or passwords for the remote administration utility or application.
- Disable remote capabilities of devices or device accounts if remote access is not employed by the agency.

2.0 Purpose and Objectives

As employees utilize remote access connectivity to conduct business within and amongst the State of Nebraska networks, security becomes increasingly at risk. These standards are designed to minimize the potential exposure from damages which may result from unauthorized use of resources; which include loss of sensitive or confidential data, intellectual property, damage to public image or damage to critical internal systems, etc. The purpose of this document is to define standards for agencies that connect from any State of Nebraska network or device to any State of Nebraska network or device.

Objectives include:

- Provide guidance to State of Nebraska agencies employees, contractors, vendors and any other agent that access any State of Nebraska network or device.
- Provide a high level of security through industry standards and best practices.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for remote access control.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0. All existing Agencies utilizing non-standard remote access applications must convert to the standard listed in Section 1.0 as soon as fiscally prudent, unless the application is exempt.

3.2 Exemption

Exemptions may be granted by the NITC Technical Panel upon request by an agency.

3.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a "Request for Exemption" to the NITC Technical Panel. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to

the Office of the NITC via e-mail. The NITC Technical Panel will consider the request and grant or deny the exemption. A denial of an exemption by the NITC Technical Panel may be appealed to the NITC.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State Agencies

Each state agency will be responsible for developing a process that ensures that secure remote access to internal State resources is maintained, and/or implemented, including but not limited to following appropriate best practices in a manner consistent with this standard and other state agency security policies.

5.0 Definitions

5.1 Principle of Least Privilege

The principle of least privilege requires that a user be given no more privilege (authority) than necessary to perform a job.

6.0 Related Documents

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
6.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)
6.3 NITC Remote Access Standard (http://www.nitc.state.ne.us/standards/index.html)
6.4 NITC Acceptable Use Policy (http://www.nitc.state.ne.us/standards/network/aup_20040309.pdf) and applicable Agency acceptable Use Policies

7.0 References

7.1 National Institute Standards and Technology (NIST) Special Publication, 800-46, “Security for Telecommuting and Broadband Communications”. (http://csrc.nist.gov/publications/nistpubs/index.html).
7.2 National Institute Standards and Technology (NIST) “Role Based Access Control” (http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html)